

CLAIMS:

Sub
a1

1 1. A method of updating a communications key maintained in a unit for
2 communicating with a communications system, said method comprising:
3 generating a new communications key using a secret value stored in said unit;
4 generating an update key using said secret value stored in said unit;
5 performing an authentication using said update key; and
6 updating said communications key with said new communications key after
7 said authentication.

1 2. The method of claim 1 comprising:
2 receiving an update sequence;
3 generating said new communications key using a secret value stored in said
4 unit and said sequence;
5 generating a signature value using said update key; and
6 comparing said signature value with a signature value received from said
7 communications system which was generated using said update key to perform said
8 authentication.

1 3. The method of claim 2 further comprises:
2 generating a challenge sequence;
3 sending said challenge sequence to said communications system;
4 generating said signature value using said challenge sequence and said update
5 key;
6 receiving a signature string generated by said communications system using
7 said challenge sequence and said update key; and
8 comparing said signature value with said signature value generated by said
9 communications system.

1 4. The method of claim 3 comprises:
2 generating a second signature value using said update sequence and said
3 update key; and
4 sending said second signature value to said communications system for
5 comparison with a second signature value generated by said communications system
6 using said sequence and said update key generated at said communications system.

1 5. The method of claim 3 wherein said generating said signature value
2 includes:
3 developing a signature string comprising at least portions of said update
4 sequence, said challenge sequence and said update key; and
5 generating said signature value from at least said signature string.

1 6. The method of claim 4 wherein said generating said signature value
2 includes:
3 developing a second signature string comprising at least portions of said
4 update sequence, said challenge sequence and said update key; and
5 generating said second signature value from at least said second signature
6 string.

1 7. A method of updating a communications key maintained in a unit and
2 in a communications system, said method comprising:
3 sending to said unit an update sequence for said unit to generate a new
4 communications key using a secret value in said unit;
5 sending to said unit a signature value for said unit to compare said signature
6 value generated at said communications system using an update key derived from a
7 secret value stored in said communications system associated with said unit; and
8 receiving an update confirmation after which said communications key is
9 updated with said authentication.

1 8. The method of claim 7 comprising:
2 generating said signature value.

1 9. The method of claim 8 wherein said generating a signature value
2 including:
3 receiving a challenge sequence from said unit; and
4 generating said signature value using said challenge sequence and said update
5 key.

1 10. The method of claim 9 including:
2 generating a second signature value using said update sequence and said
3 update key; and
4 receiving a second signature value generated at said unit using said update
5 sequence and said update key at said unit;
6 comparing with said second signature value with said second signature value
7 generated by said unit.

1 11. The method of claim 10 wherein said generating a signature value
2 including:
3 developing a signature string comprising at least portions of said update
4 sequence, said challenge sequence and said update key; and
5 generating said signature value from at least said signature string.

1 12. The method of claim 10 wherein said generating a second signature
2 value including:
3 developing a second signature string comprising at least portions of said
4 update sequence, said challenge sequence and said update key; and
5 generating said second signature value from at least said second signature
6 string.

1 13. A method of updating a communications key maintained in a unit and
2 in a communications system, said method comprising:

3 generating an update sequence; and

4 generating a new communications key using a secret value stored in said
5 communications system and associated with said unit and said update sequence;

6 generating an update key using said secret value and said update sequence;

7 updating said communications key with said new communications key after
8 an authentication is performed with said unit using said update key.

1 14. The method of claim 13 further comprising:

2 providing said update key to generate a signature value using said update key
3 in said communications system to compare at said unit said signature value with a
4 signature value generated at said unit using an update key generated at said unit using
5 said update sequence and a secret value stored in said unit; and

6 updating said communications key with said new communications key after
7 receiving the results of said comparison of said signature values.

1 15. A method of updating a communications key maintained in a unit and
2 in a home communications system, said method comprising:

3 receiving an update sequence from said home communications system for said
4 unit to generate a new communications key using a secret value in said unit;

5 receiving an update key from said from said home communications system
6 and generated at said home communications system using a secret value associated
7 with said unit at said home communications system;

8 performing an authentication with said unit using said update sequence; and

9 sending to said home communications system the results of said
10 authentication.